THE HONORABLE TANA LIN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

JACQ NIENABER, on behalf of herself and all others similarly situated,

Plaintiff,

v.

OVERLAKE HOSPITAL MEDICAL CENTER,

Defendant.

NO. 2:23-cv-01159-TL

**DEFENDANT OVERLAKE HOSPITAL MEDICAL CENTER'S MOTION TO DISMISS UNDER RULE 12(B)(6)**

NOTE ON MOTION CALENDAR: NOVEMBER 3, 2023

WITH ORAL ARGUMENT



BAKER & HOSTETLER LLP
999 Third Avenue, Suite 3900
Seattle, WA 98104-4076
Telephone: (206) 332-1380

## TABLE OF CONTENTS





BAKER & HOSTETLER LLP
999 Third Avenue, Suite 3900
Seattle, WA 98104-4076
Telephone: (206) 332-1380

## TABLE OF AUTHORITIES

**Page(s)**

**Federal Cases**





BAKER & HOSTETLER LLP
999 Third Avenue, Suite 3900
Seattle, WA 98104-4076
Telephone: (206) 332-1380

BAKER & HOSTETLER LLP
999 Third Avenue, Suite 3900
Seattle, WA 98104-4076
Telephone: (206) 332-1380

BAKER & HOSTETLER LLP
999 Third Avenue, Suite 3900
Seattle, WA 98104-4076
Telephone: (206) 332-1380

**State Cases**





BAKER & HOSTETLER LLP
999 Third Avenue, Suite 3900
Seattle, WA 98104-4076
Telephone: (206) 332-1380

**Statutes**



**Rules**





BAKER & HOSTETLER LLP
999 Third Avenue, Suite 3900
Seattle, WA 98104-4076
Telephone: (206) 332-1380

## I. INTRODUCTION

Defendant Overlake Hospital ("Overlake") respectfully moves this Court for an order dismissing Plaintiff's Class Action Complaint ("Complaint") pursuant to Federal Rule of Civil Procedure ("Rule") 12(b)(6).

In her Complaint, Plaintiff Jacq Nienaber claims that Overlake installed commonly used web-browsing analytics technologies called the Meta Pixel and Conversions API ("CAPI") on its public-facing website. Plaintiff notably does *not* allege facts showing that these technologies were installed in Overlake's secure patient portal (because it was not), an online platform that allows patients to access portions of their health information. Plaintiff only alleges facts showing that her alleged browsing activity on the public website[1] was transmitted to Meta Platforms, Inc. ("Meta").

Plaintiff's Complaint should be dismissed for failure to state a claim under Rule 12(b)(6). Another court within the Ninth Circuit recently granted a motion to dismiss each claim in a virtually identical case, holding as a threshold matter: "***Plaintiffs cannot maintain their claims based upon the theory that Defendant's sharing of their browsing activity, collected on its publicly facing website, is a disclosure of their sensitive medical information***." *Cousin v. Sharp Healthcare*, No. 22-CV-2040-MMA (DDL), 2023 WL 4484441 at *3 (S.D. Cal. Jul. 12, 2023) (emphasis added).

Plaintiff has separately failed to allege facts sufficient to plausibly satisfy the elements of each of her ten (10) claims, for at least the following reasons.

1. The negligence claim fails because (a) there is no recognized duty for safeguarding online browsing information; (b) no facts pled show any breach or disclosure of medical information; (c) there are no cognizable damages on the face of the complaint; and (d) the economic loss rule bars this claim.

2. The invasion of privacy claim fails because (a) there can be no intrusion upon seclusion because the alleged intrusion, if any, was carried out by a third party, Meta, and

[1] Plaintiff mentions the "Overlake Patient Portal" but pleads no facts regarding the Pixel or CAPI in regard to it. *See* Compl. ¶¶ 2, 228, 232, 255. In fact, Plaintiff appears to have blindly copied and pasted from other complaints, citing to irrelevant Minnesota and Arizona statutes. *See, e.g.*, *id.* ¶¶ 161, 199.



BAKER & HOSTETLER LLP
999 Third Avenue, Suite 3900
Seattle, WA 98104-4076
Telephone: (206) 332-1380

(b) Plaintiff fails to plead facts showing that Overlake engaged in any "highly offensive" conduct by installing commonly used web-browsing analytics technologies on its public website.

3. The breach of confidence claim fails because (a) there is no such cause of action, and (b) regardless, there is no breach because Plaintiff does not plead facts showing any medical information was disclosed.

4. The breach of implied contract claim fails because (a) Plaintiff fails to plead facts showing mutual assent and consideration, and (b) a privacy policy designed to be compliant with HIPAA does not give rise to a contract breach.

5. The unjust enrichment claim fails because (a) Plaintiff's provision of information and interaction with Overlake's website does not constitute conferring a benefit upon Overlake; (b) Plaintiff does not plead facts demonstrating any "unjust" outcome here; and (c) regardless, Plaintiff has already pled several theories at law.

6. The Electronic Communications Privacy Act ("ECPA") claim fails because (a) there is no civil liability for procuring an interception by a third party; (b) the ECPA is a one-party consent statute, and since Overlake was a party to the alleged "communication," it cannot be held liable for any alleged "interception"; (c) no substantive "contents" of communications are alleged to be disclosed; and (d) no alleged "device" is at issue here, just software.

7. The second ECPA claim for "unauthorized divulgence by electronic communications service" fails for the same reasons and because Overlake is not an electronic communications service provider.

8. The third ECPA claim under the Stored Communications Act fails for the same reasons.

9. The Computer Fraud and Abuse Act ("CFAA") claim fails because (a) Plaintiff does not plead facts showing that Overlake "exceeded authorized access" to her computer; (b) Plaintiff does not allege actual damage or loss to her computer; and (c) Plaintiff does not plead facts showing "threat to public health or safety."

10. Finally, the Washington Consumer Protection Act ("WCPA") claim fails because



BAKER & HOSTETLER LLP
999 Third Avenue, Suite 3900
Seattle, WA 98104-4076
Telephone: (206) 332-1380

Plaintiff does not plead facts showing that (a) she sustained injuries to her "business or property"; (b) in fact, her browsing data is not even her own property, as a recent Court of Appeals decision made clear; (c) regardless, Plaintiff does not allege facts showing that she intended to sell her healthcare/personal information on any market.

Accordingly, Overlake respectfully moves the Court to dismiss Plaintiff's Complaint *with prejudice* under Rule 12(b)(6).

## II. STATEMENT OF FACTS

Defendant Overlake is a nonprofit healthcare organization that owns and operates Overlake Hospital Medical Center in Bellevue, Washington. *See* Compl. ¶ 43. Overlake maintains the public website www.overlakehospital.org. *Id*. ¶¶ 2, 43-44. The Overlake public website provides a wide variety of information and conveniences to patients, families, employees, medical professionals, medical students, charitable donors, and the public at large. *Id*.

Speculating about a hypothetical plaintiff (not herself), Plaintiff alleges that code on Overlake's public website permits certain information to be transmitted to Meta through the Meta Pixel and Conversions Application Programming Interface ("CAPI"). *Id*. ¶¶ 3-8, 74. Plaintiff notably does ***not*** allege facts showing that the Pixel was embedded on the private patient portal, a secure online platform that allows patients to access portions of their health information. Plaintiff merely provides hypothetical "examples" of information that allegedly ***could*** be disclosed to Facebook (*id.* ¶¶ 90-103). Plaintiff also alleges she can identify hypothetical users of Overlake's website through the use of Facebook ID, cookies, and browser identifier. *Id*. ¶¶ 87-88.

Plaintiff also freely uses the word "communications" throughout the Complaint, giving the impression that actual patient-doctor communications could theoretically be shared with Meta. Tellingly, Plaintiff does not go so far as to allege facts showing that the contents of any of *her* patient-doctor communications have ever been disclosed to Meta. Rather, Plaintiff has carefully crafted her Complaint to suggest that her sensitive information was transmitted to Meta, without actually identifying what specific information was transmitted. At most, Plaintiff has alleged merely that information transmitted identifies the pages and certain content from those pages on



BAKER & HOSTETLER LLP
999 Third Avenue, Suite 3900
Seattle, WA 98104-4076
Telephone: (206) 332-1380

Overlake's public website that a hypothetical user visited. *Id.* ¶¶ 90-103.

As to herself, Plaintiff alleges that she is "a current patient of Overlake" and "used the Website numerous times . . . [to] request and schedule appointments, communicate with healthcare professionals, complete medical forms, and request and review healthcare and billing records." *Id.* ¶¶ 35-37. Plaintiff does not identify any specific sensitive information of hers that was transmitted to Meta. Instead, she summarily alleges that her "Private Information was disclosed to Facebook, and this data included her PII, PHI, and related confidential information." *Id.* ¶ 35.

Based on those allegations, Plaintiff attempts to assert ten (10) causes of action: (1) negligence; (2) invasion of privacy; (3) breach of confidence; (4) breach of implied contract; (5) unjust enrichment; (6) violation of ECPA – "unauthorized interception, use, and disclosure"; (7) violation of ECPA – "unauthorized divulgence by electronic communications service"; (8) violation of ECPA – "Stored Communications"; (9) violation of CFAA; and (10) violation of WCPA. Plaintiff seeks to broadly represent a putative class of "[a]ll individuals residing in the United States whose Private Information was disclosed to a third party without authorization or consent as a result of using Defendant's Website." *Id.* ¶ 138.

## III. LAW AND ARGUMENT

### A. Legal Standard

Federal Rule of Civil Procedure 12(b)(6) provides for dismissal if a complaint fails to state a claim upon which relief can be granted. To survive a motion to dismiss, the complaint "must contain sufficient 'well-pleaded, nonconclusory factual allegation[s],' accepted as true, to state 'a plausible claim for relief.'" *Beckington v. Am. Airlines, Inc.*, 926 F.3d 595, 604 (9th Cir. 2019) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 679-80 (2009)). Factual allegations must be enough to raise a right to relief above the speculative level. *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007). Dismissal is appropriate when the complaint lacks a "cognizable legal theory" or sufficient factual allegations to "support a cognizable legal theory." *Depot, Inc. v. Caring for Montanans, Inc.*, 915 F.3d 643, 652-53 (9th Cir. 2019).



BAKER & HOSTETLER LLP
999 Third Avenue, Suite 3900
Seattle, WA 98104-4076
Telephone: (206) 332-1380

**B. Public Website Browsing Activity is Not Actionable.**

As a threshold matter, stripped of conclusory keywords like "communications" and "personal health information," this case is about public website browsing activity only. The Southern District of California recently saw through the façade and held: "Plaintiffs cannot maintain their claims based upon the theory that Defendant's sharing of their browsing activity, collected on its publicly facing website, is a disclosure of their sensitive medical information." *Sharp Healthcare*, 2023 WL 4484441 at *3; *Smith v. Facebook*, 262 F. Supp. 3d 943, 954 (N.D. Cal. 2017), aff'd, 745 F. App'x 8 (9th Cir. 2018) ("Information available on publicly accessible websites stands in stark contrast to the personally identifiable patient records and medical histories protected by these statutes."). This Court should adopt the reasoning of this persuasive decision within the Ninth Circuit and dismiss each of Plaintiff's claims.

**C. Plaintiff Fails to State a Negligence Claim (Count I).**

To state a claim for negligence, a plaintiff must establish duty, breach, injury and proximate causation. *Lowman v. Wilbur*, 178 Wn. 2d 165, 170, 309 P.3d 387, 390 (2013). Because Plaintiff fails to establish duty, breach, and cognizable damages, and because the claim is otherwise barred by the economic loss rule, the Court should dismiss the negligence claim.

First, there is no recognized duty under Washington law for safeguarding online browsing information. To the extent Plaintiff's negligence claim is predicated upon the Health Insurance Portability and Accountability Act ("HIPAA"), this federal statute is administrative in nature—it provides rules for hospital systems to conform to or face administrative penalties. *See generally* Pub. L. 104–191, 110 Stat. 1936. It does not permit a private cause of action and, therefore, cannot be found to establish any duty owed by Overlake to Plaintiff. *See Webb v. Smart Document Sols., LLC*, 499 F.3d 1078, 1080 (9th Cir. 2007); *see also Towles v. Dzurenda*, 735 Fed. Appx. 440, 440 (9th Cir. 2018) (finding the district court properly dismissed claim alleging HIPAA violations because "there is no private right of action under the statute."); *Seaton v. Mayberg*, 610 F.3d 530, 533 (9th Cir. 2010) (same); *Wilkerson v. Shinseki*, 606 F.3d 1256, 1267 n.4 (10th Cir. 2010) (finding HIPAA does not create a private right of action for alleged disclosures of confidential



BAKER & HOSTETLER LLP
999 Third Avenue, Suite 3900
Seattle, WA 98104-4076
Telephone: (206) 332-1380

medical information); *In re MCG Health Data Sec. Issue Litig.*, No. 2:22-CV-849-RSM-DWC, 2023 WL 3057428, at *3 (W.D. Wash. Mar. 27, 2023), report and recommendation adopted, No. 2:22-CV-849-RSM-DWC, 2023 WL 4131746 (W.D. Wash. June 22, 2023) ("To the extent that HIPAA universally has been held not to authorize a private right of action, to permit HIPAA regulations to define per se the duty and liability for breach is no less than a private action to enforce HIPAA, which is precluded."); *Doe v. Meta Platforms, Inc.*, No. 22-cv-03580-WHO, 2023 WL 5837443, at *13 (N.D. Cal. Sept. 7, 2023) (dismissing negligence per se claim based on an alleged duty created by HIPAA.); *Teeter v. Easterseals-Goodwill N. Rocky Mountain, Inc.*, No. CV-22-96-GF-BMM, 2023 WL 2330241, at *4 (D. Mont. Mar. 2, 2023) (same). Accordingly, HIPAA cannot form the basis for any duty owed by Overlake toward Plaintiff. No other cognizable duty is available here.

Second, even if Plaintiff had established any cognizable duty, she has failed to establish any breach. There are no facts pled (as opposed to conclusions) showing that anyone's (let alone Plaintiff's) medical records have been disclosed to any third party. There are no facts pled showing that a single diagnosis, treatment, or medication has been disclosed to any third party.

Finally, Plaintiff fails to allege any cognizable damages because she (a) does not plead facts showing that she lost the opportunity to sell her information or that the value of their information was somehow diminished after it was collected by Facebook (*In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 930-31 (N.D. Cal. 2015)); (b) cannot otherwise recover on an overpayment theory (*Lovell v. P.F. Chang's China Bistro, Inc.*, No. C14-1152RSL, 2015 WL 4940371, at *2 (W.D. Wash. Mar. 27, 2015)); and (c) to the extent Plaintiff seeks to recover damages related to "anxiety arising from a current reasonable fear of future injury or illness, and resulting from an injury caused by the defendant," anxiety is only compensable if the plaintiff is able to show "with reasonable probability" that she will actually suffer the feared harm. *Koker v. Armstrong Cork, Inc.*, 60 Wn. App. 466, 482, 804 P.2d 659, 669 (1991). Plaintiff makes no such showing.



BAKER & HOSTETLER LLP
999 Third Avenue, Suite 3900
Seattle, WA 98104-4076
Telephone: (206) 332-1380

**D. Plaintiff Fails to State an Invasion of Privacy Claim (Count II).**

Plaintiff may sue for common law invasion of privacy if the defendant intentionally intrudes on his or her solitude, seclusion or private affairs. *Youker v. Douglas Cty*., 178 Wn. App. 793, 797, 327 P.3d 1243, 1245 (2014). The defendant's intrusion must substantially interfere with plaintiff's seclusion in a highly offensive or objectionable to a reasonable person. *Id*.

There can be no intrusion here because the alleged intrusion, if any, was carried out by a third party, Meta. *Poore-Rando v. U.S.*, C16-5094 BHS, 2017 WL 5756871, at *2 (W.D. Wash. Nov. 28, 2017) ("[A]n actor commits an intentional intrusion only if he believes, or is substantially certain, that he lacks the necessary legal or personal permission to commit the intrusive act.") (citations and quotations omitted). In dismissing the plaintiff's virtually identical intrusion upon seclusion claim, the *Kurowski* court explained: "The question is therefore whether Kurowski has alleged sufficient facts to allow an inference that [the health care provider] intruded upon its patients' seclusion when it allowed third-party source code to collect the data Kurowski alleges it later disclosed. The Court concludes she has not." *Kurowski v. Rush Sys. For Health*, No. 22 C 5380, 2023 WL 2349606, at *9 (N.D. Ill. Mar. 3, 2023). The court elaborated:

> It is clear from Kurowski's complaint that the core of her claim is Rush's deployment of third-party source code that causes the transmission of patient data. As discussed with respect to count 1, the allegedly intercepted communications were intended to reach Rush. This is underscored by the theme underlying most of Kurowski's allegations, namely, that patients trusted that communications and queries directed at Rush, their health care provider, would be kept private. In other words, harm for which Rush is responsible, if any, is its disclosure of patient data (which, as alleged, is not protected private health information) – not the obtaining of that data. The actual intrusion upon patients' seclusion, via interception of their communications, is carried out by third parties.

*Id*. at 9.

Here, too, Plaintiff alleges only that Overlake's deployment of third-party source code causes the transmission of data to be disclosed to Meta. *See* Compl. ¶ 84. As in *Kurowski*, the actual alleged intrusion upon patients' seclusion, if any, is carried out by Meta, not Overlake, thus precluding an intrusion upon seclusion claim against Overlake as a matter of law. *Buckley v. Santander Consumer USA, Inc.*, No. C17-5813 BHS, 2018 WL 1532671, at *7 (W.D. Wash. Mar. 29, 2018) (dismissing intrusion upon seclusion claim where defendant possessed the necessary



BAKER & HOSTETLER LLP
999 Third Avenue, Suite 3900
Seattle, WA 98104-4076
Telephone: (206) 332-1380

legal permission to acquire plaintiff's personal information.); *see also Steinberg v. CVS Caremark Corp., et al*., 899 F. Supp. 2d 331, 342–43 (E.D. Pa. 2012) (finding no intrusion upon seclusion claim can be brought where defendant legitimately obtains information from a plaintiff, even if the facts are later disclosed to a third party). Since amendment would be futile, the claim should be dismissed with prejudice.

Separately, Plaintiff has failed to allege any conduct that is "highly offensive" to a person with ordinary sensibilities, and so, she fails to state a tort claim for invasion of privacy. *Youker*, 327 P.3d at 1245. In determining the degree of offensiveness, "courts consider, among other things: 'the degree of the intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded.'" *Deteresa v. Am. Broad. Cos*., 121 F.3d 460, 465 (9th Cir. 1997) (quoting *Hill v. Nat'l Collegiate Athletic Ass'n*, 865 P.2d 633 (1994) (en banc)); *Mark v. King Broad. Co.*, 27 Wn. App. 344, 355, 618 P.2d 512, 519 (1980) ("This form of invasion of privacy is actionable only if the interference with a plaintiff's seclusion is a substantial one resulting from conduct of a kind that would be highly offensive and objectionable to the ordinary person.") (quotation omitted).

The conduct alleged in the Complaint falls far short of this high bar. *Id*. There are no factual allegations establishing anything that Overlake may have done, or any information Overlake may have transmitted to Meta, that would demonstrate a "highly offensive . . . degree of [] intrusion," let alone allege sufficient "context" regarding the "intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded.'" *Deteresa*, 121 F.3d at 465. The crux of Plaintiff's allegations against Overlake is that it embedded Meta's proprietary tracking technology, which then allegedly used some unidentified information about users of Overlake's public website to provide advertising about services that may be of interest to her. *See generally* Compl. ¶¶ 132-35. Because Plaintiff fails to allege facts showing that Overlake engaged in highly offensive conduct, it is appropriate for the Court to dismiss this claim with prejudice. *See Hammerling v. Google LLC*, No. 21-cv-09004-CRB, 2022 WL 17365255, at **8-9



BAKER & HOSTETLER LLP
999 Third Avenue, Suite 3900
Seattle, WA 98104-4076
Telephone: (206) 332-1380

(N.D. Cal. Dec. 1, 2022) (dismissing intrusion upon seclusion claim because the tracking of plaintiff's bank, where she kept her investments, what car she drove, where she reads her news, interests, use of apps, and that she was physically active is not highly offensive.).

Similarly, in *In re Google, Inc. Privacy Policy Litig*. The Northern District of California found no highly offensive conduct when plaintiffs alleged that Google tracked their browsing data while using Google's services. 58 F. Supp. 3d 968, 987–88 (N.D. Cal. 2014). *See also Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (2012) (LinkedIn's disclosure of users' browser history to third parties was not highly offensive); *In re iPhone Application Litig*., 844 F. Supp. 2d 1040, 1060, 1063 (N.D. Cal. 2012) (disclosures of unique device identification number, personal data, and geolocation information without consent were not an egregious breach of social norms).

The *Kurowski* court also explained that a similarly situated patient's alleged online communications were "not protected private health information," even if they "identifie[d] an individual patient by name." *Kurowski*, 2023 WL 2349606 at **6, 9. On this separate ground, *Kurowski* granted the healthcare provider's motion to dismiss the plaintiff's intrusion upon seclusion claim. *Id*. at *9; *id*. at *5 ("Kurowski has not alleged sufficient facts, however, to support an inference that Rush disclosed its patients' individually identifiable health information . . ."); *id*. at *6 ("Kurowski fails to allege the disclosure of any information related to the provision of treatment to her or other similarly situated Rush patients.").

Another court recently dismissed a similar invasion of privacy claim "[b]ecause the plaintiffs acknowledge in the complaint that they voluntarily provided their information directly to the [medical provider]." *Allen v. Novant Health, Inc*., No. 1:22-CV-697, 2023 WL 5486240, at *2 (M.D.N.C. Aug. 24, 2023). This Court should do the same.

Plaintiff otherwise alleges her status as an Overlake patient and "health information" were disclosed. Compl. ¶ 32. There is no basis for concluding that disclosure of a person's status as a patient at an acute care hospital, without more, is "highly offensive." *See Sutter Health v. Super. Ct.*, 227 Cal. App. 4th 1546, 1553 (2014). Indeed, Plaintiff readily disclosed this information on the public record. Compl. ¶¶ 3, 32.



BAKER & HOSTETLER LLP
999 Third Avenue, Suite 3900
Seattle, WA 98104-4076
Telephone: (206) 332-1380

Moreover, there is no basis for inferring that the alleged disclosure of Plaintiff's "health information" is "highly offensive" because she does not allege any "health information" was disclosed. *Id*.

**E. Plaintiff Fails to State a Breach of Confidence Claim (Count III).**

"Washington has not recognized a breach of confidence as a common law cause of action." *Snapp v. Burlington N. Santa Fe Ry*., No. 10-cv-05577-RBL, 2012 WL 3157137, at *5 (W.D. Wash. Aug. 3, 2012), reversed on other grounds by *Snapp v. United Transp. Union*, 547 F.App'x 824 (9th Cir. 2013). Accordingly, the claim fails as a matter of law. Further, no Washington court has imposed a duty of confidentiality in the context of a data breach or comparable alleged privacy violation. *See In re Capital One Consumer Data Security Breach Litig.*, 488 F. Supp. 3d 374, 4409 at n.21 (E.D. Va. 2020). And as explained above, Plaintiff has not pled facts establishing any sort of breach or disclosure of personal health information.

**F. Plaintiff Fails to State a Breach of Implied Contract Claim (Count IV).**

Under Washington law, a contract implied in fact is an agreement depending for its existence on some act or conduct of the party sought to be charged and arising by implication from circumstances which, according to common understanding, show a mutual intention on the part of the parties to contract with each other. The services must be rendered under such circumstances as to indicate that the person rendering them was expected to be paid therefor, and that the recipient expected, or should have expected, to pay for them. *Johnson v. Nasi*, 50 Wn. 2d 87, 91, 309 P.2d 380, 383 (1957). Plaintiff's claim for breach of implied contract fails for multiple independent reasons.

Plaintiff fails to allege the existence of a valid contract, supported by mutual assent and consideration. *Id*. Plaintiff alleges that she entered into an unspecified contract for "services" rendered by Overlake. *See* Compl. ¶ 189. The Court should not credit such vague and conclusory allegations, containing no facts as to any "contracts," any contract terms, or any "services." *Buckley*, 2018 WL 1532671 at *7 (dismissing breach of contract claim where plaintiff failed to specify any agreement that defendant would not disclose her information to third parties).



BAKER & HOSTETLER LLP
999 Third Avenue, Suite 3900
Seattle, WA 98104-4076
Telephone: (206) 332-1380

Regardless, there is no indication that any contract included alleged promises to safeguard Plaintiff's data. *Lovell*, 2015 WL 4940371 at *7 (dismissing breach of implied contract claim where implied contract could only relate to provision and payment of food, and not data security). To the extent Plaintiff seeks to rely on her *subjective* understanding there was a contract to safeguard her data, such reliance would be insufficient. *Thompson v. St. Regis Paper Co.*, 102 Wn. 2d 219, 224, 685 P.2d 1081, 1085 (1984) (employee's "subjective understanding that he would be discharged only for cause . . . is insufficient to establish an implied contract to that effect").

Separately, Overlake's privacy policy cannot serve as an enforceable contract because multiple courts have held that a notice of privacy practices is mandated by HIPAA; accordingly, this notice is not a bargained-for contract, but rather merely the health care provider complying with federal law. *See In re Maple*, 434 B.R. 363, 371 (E.D. Va. 2010); *Thornton v. Statcare, PLLC*, 988 So. 2d 387, 392 (Miss. App. 2008); *Brush v. Miami Beach Healthcare Grp. Ltd*., 238 F. Supp. 3d 1359, 1367–69 (S.D. Fla. 2017); *J.R. v. Walgreens Boots All., Inc*., No. 2:19-CV-00446-DCN, 2020 WL 3620025, at *14 (D.S.C. July 2, 2020).

Finally, the damages Plaintiff seeks are not recoverable in contract, as courts within the Ninth Circuit have routinely held that "damages based on the collection and dissemination of personal information are insufficient to state a claim for breach of contract." *Yunker v. Pandora Media, Inc.*, No. 11-CV-03113 JSW, 2013 WL 1282980 at *13 (N.D. Cal. Mar. 26, 2013); *Low*, 900 F. Supp. 2d at 1028-29; *In re Facebook Litig.*, 791 F. Supp. 2d 705, 717 (N.D. Cal. 2011); *see also Hameed-Bolden v. Forever 21 Retail, Inc.*, No. cv-18-03019-SJO (JPRx), 2021 WL 6802818, at *8 (C.D. Cal. Oct. 1, 2018) (explaining "[a] plaintiff must plead 'appreciable and actual damages' in relation to their breach of contract claim.") (citation omitted). At most, Plaintiff has alleged that she received targeted advertising, which is not an actual injury compensable under a contract theory. Plaintiff has also failed to alleged "tangible, out-of-pocket expenses," as required by courts within the Ninth Circuit. *See Castillo v. Seagate Tech.*, No. 16-cv-01958-RS, 2016 WL 9280242, at *4 (N.D. Cal. Sept. 14, 2016); *Pruchnicki v. Envision Healthcare Corp*., 439 F. Supp. 3d 1226, 1233 (D. Nev. 2020), aff'd, 845 F. App'x 613 (9th Cir. 2021); *Hameed-Bolden*, 2021

WL 6802818 at *8.

**G. Plaintiff Fails to State an Unjust Enrichment Claim (Count V).**

To state a claim for unjust enrichment, Plaintiff must plead sufficient facts showing (1) Overlake received a benefit, (2) at Plaintiff's expense, and (3) the circumstances make it unjust for Overlake to retain the benefit without payment. *Young v. Young*, 164 Wn. 2d 477, 484, 191 P.3d 1258, 1262 (2008); *see also In re MCG Health Data Sec. Issue Litig.*, 2023 WL 3057428 at *5; *Chandler v. Washington Toll Bridge Auth.*, 17 Wn. 2d 591, 602-03, 137 P.2d 97, 102 (1943) ("A person confers a benefit upon another if he gives to the other possession of or some other interest in money, land chattels, or choses in action . . . or in any way that adds to the other's security or advantage . . . the word 'benefit,' therefore, denotes any form of advantage.") (internal quotation and citation omitted).

Plaintiff has failed to state an unjust enrichment claim because she has failed to plead facts showing that (a) Overlake received a "benefit" from Plaintiff's provision of information and interaction with Overlake's public website; (b) Plaintiff suffered any detriment; or (c) any use of Plaintiff's public website browsing data was somehow "unjust."

Plaintiff's unjust enrichment claim also fails for the same reasons as her implied breach of contract claim. *See also Heeger v. Facebook, Inc.*, 509 F. Supp. 3d 1182, 1191 (N.D. Cal. 2020) (dismissing unjust enrichment claim where plaintiffs were unable to make any allegation that "they retain a stake in the profits garnered from" the collection of their IP addresses).

**H. Plaintiff Fails To State A Claim Against Overlake For Violation Of The Electronic Communications Privacy Act ("ECPA") (Counts VI – VIII).**

A claim under the ECPA (18 U.S.C. § 2510, *et seq.*) "requires a showing that the defendant (1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication, (5) using a device." *See In re Facebook Internet Tracking Litig.*, 263 F. Supp. 3d 836, 844 (N.D. Cal. 2017) (internal quotation marks omitted). In a sleight of hand, Plaintiff attempts to segment her ECPA claim into three (3) different "counts." But each "count" requires Plaintiff to establish each of the above



BAKER & HOSTETLER LLP
999 Third Avenue, Suite 3900
Seattle, WA 98104-4076
Telephone: (206) 332-1380

elements, and Plaintiff cannot satisfy at least the second, third, or fourth elements.

Counts VI – VIII alleging a violation under the ECPA should therefore be dismissed as a matter of law, without leave to amend.

***1. Plaintiff Fails To Allege Any Unlawful Interception***

Count VI focuses on an alleged interception of communications through the Pixel. However, Plaintiff cannot establish that any communication has been unlawfully "intercepted" by Overlake. The ECPA is a one-party consent statute. 18 U.S.C. § 2511(2)(d) (The ECPA does not make it unlawful for someone to "intercept ... electronic communication where such person is a party to the communication."); *see also In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262, 275 (3d Cir. 2016) (discussing "one-party consent language in the Wiretap Act"). Stated differently, a party to a communication cannot unlawfully "intercept" a communication directed to it and cannot be held liable for "eavesdropping" upon itself. 18 U.S.C. § 2511(2)(d); *In re Nickelodeon*, 827 F.3d at 275 (dismissing ECPA claim because defendant "was either a party to all communications with the Plaintiff's computers or was permitted to communicate with the Plaintiff's computers by Viacom, who was itself a party to all such communications."); *see also In re Google Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 142–143 (3rd Cir. 2015) (dismissing ECPA claim because tracking cookies placed by advertising providers made the advertiser the intended recipient of the electronic transmission); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d at 713 (dismissing ECPA claim on same grounds).

The recent *Kurowski* decision made clear that users of a health care provider's websites could not state a claim under the ECPA because the health care provider was the intended recipient of the communication and, therefore, could not have intercepted the communication allegedly occurring on the health care provider website. 2023 WL 2349606 at *4 ("The Court concludes that Rush [the healthcare provider]—and not Facebook, Google, or Bidtellect—was the intended recipient of the allegedly intercepted communications here. Rush is therefore a party to those communications and cannot be liable under the Wiretap Act for its alleged interception of them, if such an interception even occurred."); *see also Allen*, 2023 WL 5486240 at *4 (same ruling).

Overlake is identically situated.

While there is a statutory exception under the ECPA where a "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State," 18 U.S.C. § 2511(2)(d), this exception does not apply to the alleged interception itself; instead, "a plaintiff must plead sufficient facts to support an inference that the offender intercepted the communication for the purpose of a tortious or criminal act that is *independent* of the intentional act of recording." *In re Google Cookie Placement*, 806 F.3d at 145 (emphasis in original, quoting *Caro v. Weintraub*, 618 F.3d 94, 100 (2d Cir. 2010)).

Plaintiff's ECPA claim against Overlake is tethered to the alleged transmission of browsing activities on the Overlake public website, not any other independent tortious or criminal act. *See, e.g.,* Compl. ¶ 211 (alleging Overlake "intercepted" alleged communications "via the Pixel"). Although Plaintiff contends that her ECPA claim should survive under Section 2511(2)(d), the *Kurowski* court flatly rejected such a theory. 2023 WL 2349606 at *4 ("The 'exception' to the party exception for criminal or tortious intent does not apply."). This Court should do the same, especially since Plaintiff does not plead facts showing any tortious or criminal *use* of the alleged intercepted communications. *Id.*; *see also In re Google Cookie Placement*, 806 F.3d at 145 ("As the plaintiffs plead no tortious or criminal *use* of the acquired internet histories, § 2511(d) is not inapplicable on the basis of the criminal-tortious purpose exception.") (emphasis in original).

Both the case law and the facts actually pled by Plaintiff establish that Overlake was a party to (and intended recipient of) her alleged communications on the Overlake public website. Plaintiff therefore cannot establish the second element of her ECPA claim – an unlawful interception of a communication. The claim therefore should be dismissed as a matter of law and with prejudice, as further amendment would be futile. *In re Nickelodeon*, 827 F.3d at 275; *In re Google Cookie Placement*, 806 F.3d at 142-43; *In re Facebook Priv. Litig,* 791 F. Supp. 2d at 713.



BAKER & HOSTETLER LLP
999 Third Avenue, Suite 3900
Seattle, WA 98104-4076
Telephone: (206) 332-1380

### *2. There Can Be No Civil Liability for Allegedly "Procur[ing]" or Aiding and Abetting an Alleged Interception Through the Pixel*

Plaintiff's ECPA claim further fails as a matter of law because it is dependent on allegations that Overlake "procure[d]" an alleged interception by Meta through the use of the Pixel. *See, e.g.*, Compl. ¶¶ 210, 234, 243. Indeed, all of Plaintiff's underlying allegations identify Meta – not Overlake – as the party that allegedly intercepted Plaintiff's communications through its source code on the Overlake public website. *Id*. ¶ 6. These allegations *independently warrant* dismissal of Plaintiff's ECPA claim.

The ECPA's private right of action is found in 18 U.S.C. § 2520, which creates a scope of civil liability that is narrower than the criminal liability provision codified in Section 2511. Section 2520(a)'s plain, unambiguous language creates a private civil cause of action only against the person who engages in an unlawful interception, disclosure, or intentional use of wire, oral or electronic communication – not against any other person for procuring, enabling, aiding or abetting another's interception of such. *See, e.g., Kirch v. Embarq Mgmt. Co*., 702 F.3d 1245, 1246-47 (10th Cir. 2012) (holding that there is no civil ECPA claim for "procuring" or "aiding and abetting" an interception); *see also Peavy v. WFAA-TV, Inc*., 221 F.3d 158, 169 (5th Cir. 2000) (same). When Congress enacted the ECPA in 1986, it specifically excluded civil liability for procurement (or aiding and abetting), which previously existed under the 1968 predecessor to the ECPA. *See Kirch*, 702 F.3d at 1246-47 (addressing the statutory distinctions between civil and criminal liability under the ECPA).

Courts within the Ninth Circuit are in accord. *In re Toys R Us, Inc., Privacy Litig*., No. 00-CV-2746, 2001 WL 34517252, at *7 (N.D. Cal. Oct. 9, 2001) ("The Court finds that § 2520(a) does not provide a cause of action against aiders and abetters, and, accordingly, that plaintiffs may not proceed against Toys R Us on such theory."); *In re Carrier IQ, Inc., Consumer Privacy Litig*., 78 F. Supp. 3d 1051, 1089 (N.D. Cal. 2015) (explaining "there is simply no secondary liability (such as aiding and abetting) under the ECPA.").

Because the ECPA does not provide a private cause of action against an entity that is



BAKER & HOSTETLER LLP
999 Third Avenue, Suite 3900
Seattle, WA 98104-4076
Telephone: (206) 332-1380

alleged to have procured or aided and abetted another party to intercept a communication, Plaintiff's ECPA claim should be dismissed as a matter of law.

***3. Plaintiff Fails To Allege Any Plausible Interception of "Contents"***

Plaintiff's ECPA claim further fails because Plaintiff has not pled facts showing that the "contents" of any communications were disclosed to Meta—the third element of her claim. Under the ECPA, the "contents" of a communication are defined as "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). Courts distinguish between "content" and "record" information. *See In re Zynga Privacy Litig.*, 750 F.3d 1098, 1106–07 (9th Cir. 2014) (in the ECPA "the term 'contents' refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication" such as a name, address, or the identity of a subscriber or customer).

In *Facebook Internet Tracking Litig.*, the court held that a URL sent to Meta by a user's browser does not qualify as "contents" of a "communication" under the ECPA because it is nothing more than "record information regarding the characteristics of the message that is generated in the course of the communication.'" 140 F. Supp. 3d at 935 (quoting *In re Zynga*, 750 F.3d at 1106–07). The court emphasized that "[p]laintiff may never be able to state [a] Wiretap Act claim, particularly since their arguments on this issue are so unpersuasive." *Id.* By definition, a URL does not convey the "meaning" of the communication with the host server; it simply identifies the location of the requested webpage on the Internet. In *Zynga,* the Ninth Circuit explained that a URL could disclose that a person viewed the "page of a gay support group," yet the court still held that such URLs "function[] like an 'address,'" not "contents" of a communication. 750 F.3d at 1107. *See also Sharp Healthcare*, 2023 WL 4484441 at *9 (relying on *Zynga* and dismissing California wiretap act claim—which as a matter of law is analyzed in the same way as an ECPA claim—on the ground that "Plaintiffs do not provide sufficient factual support to plausibly claim their content was intercepted by Meta as a result of installing Meta Pixel on Sharp's webpage.").

Here, Plaintiff's Complaint fails to allege any facts showing that the substantive contents



BAKER & HOSTETLER LLP
999 Third Avenue, Suite 3900
Seattle, WA 98104-4076
Telephone: (206) 332-1380

of her (or anyone's) alleged communications have ever been transmitted to Meta. Plaintiff parroting the legal conclusion that patients' "medical information" or "patient health information" are transmitted to Google, without alleging any facts in support (*see, e.g.,* Compl. ¶¶ 1-2, 5), is insufficient as a matter of law. *See, e.g., Iqbal*, 556 U.S. at 678 (mere conclusions are insufficient); *see also Burtch v. Milberg Factors, Inc.*, 662 F.3d 212, 225 (3d Cir. 2011) (rejecting allegations that the defendant "regularly and unlawfully shared highly confidential information" related to customers as conclusory in nature); *Rodriguez v. Google LLC*, No. 20-CV-04688-RS, 2022 WL 214552, at *2 (N.D. Cal. Jan. 25, 2022) ("Using the word 'intercept' repeatedly is simply not enough without the addition of specific facts that make it plausible Google is intercepting their data in transit.").

#### *4. Overlake Is Not A Provider Of An "Electronic Communication Service" Under Section 2511(3)(a) Of The ECPA*

Counts VII appear to be premised on an alleged violation of Section 2511(3)(a) of the ECPA. *See* Compl. ¶ 222. Section 2511(3)(a) prohibits the provider of an "electronic communication service" from divulging the content of communications transmitted on that service to third parties (*i.e.*, anyone other than the intended recipient). 18 U.S.C. § 2511(3)(a). Plaintiff alleges that Overlake is an "electronic communication services [sic]" or a "conduit" in regard to the public website (Compl. ¶¶ 224-26), and that Overlake intentionally caused the contents of Plaintiff's electronic communications with Overlake to be "divulge[ed]" to Meta. *Id.* ¶¶ 234-35.

Plaintiff's claim under this provision fails for two independent reasons. ***First***, as numerous courts have held, "[a] company that merely utilizes electronic communications in the conduct of its own business is generally considered a purchaser or user of the communications platform, not the provider of the service to the public." *Garner v. Amazon.com, Inc.*, 603 F. Supp. 3d 985, 996 (W.D. Wash. 2022) (rejecting argument that Amazon's "Alexa" was an electronic communications service); *see also In re Jetblue Airways Corp. Priv. Litig.*, 379 F. Supp. 2d 299, 307–08 (E.D.N.Y. 2005) (rejecting the argument Jetblue Passenger Reservation Systems' constituted an electronic communications service; "companies that provide traditional products and services over the

Internet, as opposed to Internet access itself, are not 'electronic communication service' providers within the meaning of the ECPA"); *Casillas v. Cypress Ins. Co.*, 770 F. App'x 329, 331 (9th Cir. 2019) (same holding where defendant's HQ Sign-Up Services "does not permit users to communicate directly with each other").

Most recently, the *Kurowski* court explained that a healthcare provider "cannot plausibly be considered an electronic communications service provider within the meaning of the [ECPA]." 2023 WL 2349606 at *6. In *Kurowski*, the plaintiff alleged that, "by providing access to the MyChart patient portal – which allows patients to communicate directly with their providers – Rush [the health care provider] acts as an electronic communication service," which the court rejected. *Id.* at *5-6. Plaintiff here makes similar allegations regarding the Overlake public website. *See* Compl. ¶¶ 224, 241, 243,257. This Court should similarly reject Plaintiff's argument that Overlake is an electronic communication service provider under Section 2511(3)(a).

***Second***, as addressed above, Plaintiff does not allege facts showing that the "contents" of any of *her* alleged communications were disclosed to Meta. Plaintiff's general allegations say nothing about the specific contents of any alleged Internet communication she may have had with Meta, or how any such communications were actually divulged to Meta.

***5. For The Same Reasons, Overlake Is Not A Provider Of An "Electronic Communications Service" Under Section 2702(a)(1) Of The ECPA***

Count IV appears to be a claim under the Stored Communications Act (SCA) of the ECPA, 18 U.S.C. § 2702(a)(1). The SCA does not apply to Overlake because, again, as a healthcare provider, Overlake merely provides access to its public website in the conduct of its own business (not a communications service to the public). *Kurowski*, 2023 WL 2349606 at *6; *Garner*, 603 F. Supp. 3d at 996; *Jetblue Airways*, 379 F. Supp. 2d at 307–08; *Casillas*, 770 F. App'x at 331; *see also Dyer v. Nw. Airlines Corps.*, 334 F. Supp. 2d 1196, 1199 (D.N.D. 2004) ("Northwest Airlines is not an electronic communications service provider as contemplated by the ECPA … businesses offering their traditional products and services online through a website are not providing an 'electronic communication service'"); *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1270

(N.D. Cal. 2001) (rejecting the argument that an online retailer that merely receives emails provides an electronic communication service under the ECPA); *Pica v. Delta Air Lines, Inc*., No. CV 18-2876-MWF (EX), 2019 WL 1598761, at *6–7 (C.D. Cal. Feb. 14, 2019), aff'd, 812 F. App'x 591 (9th Cir. 2020) ("[T]he Court is persuaded that, although Plaintiffs allege that Delta operates a website and computer servers, there are no facts alleged [to] indicate that Delta 'provides either computer processing services or computer storage to the public' under the plain meaning of the SCA") (citations omitted).

## I. Violation of CFAA (Count IX).

Liability under the CFAA may attach when someone "intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains information containing in a financial record of a financial institution, information from any department or agency of the United States, or information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). "Exceeds authorized access" means "to access with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). This does not cover those who have improper motives for obtaining information that is otherwise available to them. *Van Buren v. United States*, 141 S. Ct. 1648, 1652 (2021). The CFAA's civil liability provision codified at 18 U.S.C. § 1030(g) limits any civil action under section 1030 to a "person who suffers damage or loss by reason of a violation of this section."

Plaintiff's CFAA claim should be dismissed for failure to plead the basic element of "exceed[ing] authorized access." 18 U.S.C. § 1030(a)(2)(C). Plaintiff does not allege that Overlake did not have authorization to access her computer. Instead, she conclusively asserts that Overlake "exceeded its unauthorized access because Defendant accessed Plaintiff's and Class Members' Private Information under false pretenses, *i.e*., Defendant did not disclose it was transmitting Private Information to Facebook." Compl. ¶ 262. The Supreme Court narrowly interpreted the provision as follows: "[A]n individual 'exceeds authorized access' when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off limits to him." *Van Buren*, 141 S. Ct. at 1662. The



BAKER & HOSTETLER LLP
999 Third Avenue, Suite 3900
Seattle, WA 98104-4076
Telephone: (206) 332-1380

Supreme Court rejected a broad interpretation that would effectively "criminalize [] every violation of a computer-use policy" because "then millions of otherwise law-abiding citizens are criminals." *Id.* at 1661. Plaintiff does not allege that Overlake's website servers obtained information from other parts of her computer to which the servers were not otherwise authorized to access. The claim fails as a matter of law.

Separately, Plaintiff has failed to plead facts establishing any "loss," as that term is specifically defined in the CFAA to mean direct costs incurred in responding to a violation. 18 U.S.C. § 1030(e)(11); *see also id.* at § 1030(g) ("Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages."). Even allegations that a defendant "hacked" information "valued at over $5,000" is insufficient because "those are not 'losses' under the CFAA." *Schwartz v. ADP, Inc.*, Case No. 21-cv-283, 2021 WL 5760434, at *2 (M.D. Fla. Dec. 3, 2021). "The statutory definitions of 'damage' and 'loss' thus focus on technological harms—such as the corruption of files—of the type unauthorized users cause to computer systems and data. Limiting 'damage' and 'loss' in this way makes sense in a scheme 'aimed at preventing the typical consequences of hacking.'" *Van Buren*, 141 S. Ct. at 1659-60.

Moreover, the conclusory statement that using the Pixel or CAPI on a public website "constitutes 'a threat to public health or safety' under 18 U.S.C. § 1030(c)(4)(A)(i)(IV)" is insufficient. Plaintiff fails to support with any facts whatsoever how use of the Pixel or CAPI on a public website raises to the level of the "public health or safety threat" contemplated by a statute targeted at computer hacking and cybercriminals.

**J. Violation of WCPA (Count X).**

The WCPA provides that "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful." RCW 19.86.020. To prevail on a private CPA claim, plaintiffs must prove (1) an unfair or deceptive act or practice, (2) occurring in trade or commerce, (3) affecting the public interest, (4) injury to a person's business or property, and (5) causation. *Hangman Ridge Stables, Inc. v. Safeco Title Ins. Co.*, 105 Wn. 2d 778,784, 719 P.2d 531, 535 (1986).



BAKER & HOSTETLER LLP
999 Third Avenue, Suite 3900
Seattle, WA 98104-4076
Telephone: (206) 332-1380

Here, Plaintiff has failed to establish injury to her business or property. Personal injuries, as opposed to injuries to business or property, are not compensable and do not satisfy the injury requirement for a claim for unfair or deceptive conduct under Washington's Consumer Protection Act. *Robertson v. GMAC Mortg. LLC*, 982 F. Supp. 2d 1202, 1209 (W.D. Wash. 2013), affirmed on other grounds 702 Fed. App'x. 595 (2017), *certiorari denied* 138 S. Ct. 1289, 200 L. Ed. 2d 472 (2018); *see also Dinerstein v. Google, LLC*, 73 F.4th 502, 518 (7th Cir. 2023) (finding a patient does not have a property interest in their medical records; "they instead belong to the medical provider."); *Doe v. Meta Platforms, Inc.*, 2023 WL 5837443 at *15 (in analyzing whether the plaintiffs had been damaged in their "property" under California's Unfair Competition Law ("UCL") the court explained, "[c]ourts in this district have dismissed cases where, like here, the injury is based on the loss of the inherent value of their personal data.") (internal citations and quotations omitted). Accordingly, the WCPA claim should be dismissed without leave to amend.

Finally, even if the value of Plaintiff's healthcare information somehow qualifies as lost property (it does not), there are no allegations that she intended to participate in that market. Courts have also routinely rejected the "loss of value in PII" theory of injury when the plaintiff, like Plaintiff here, does not "contend that [they] intended to sell this information on the cyber black market in the first place" and does not provide any facts as to "whether or how the data has been devalued by the breach." *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.* ("SAIC"), 45 F. Supp. 3d 14, 30 (D.D.C. 2014); *Corona v. Sony Pictures Entm't, Inc.*, No. 14-CV-09600 RGK EX, 2015 WL 3916744, *4 (C.D. Cal. June 15, 2023) (rejecting claim that "an individual's personal identifying information has any compensable value in the economy at large"); *Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d 735, 755 (W.D.N.Y. 2017) ("Courts have routinely rejected the proposition that an individual's personal identifying information has an independent monetary value."); *Khan v. Children's Nat'l Health Sys.*, 188 F. Supp. 3d 524, 531 (D. Md. 2016) (rejecting, in standing context, diminution in value theory because plaintiff did not "explain how the hackers' possession of that information ha[d] diminished its value, nor d[id] she assert that she would ever actually sell her own personal information"); *Green v. eBay Inc.*, No.



BAKER & HOSTETLER LLP
999 Third Avenue, Suite 3900
Seattle, WA 98104-4076
Telephone: (206) 332-1380

14–1688, 2015 WL 2066531, at *5 n.5 (E.D. La. May 4, 2015) (finding, in the standing context, that "[e]ven if the Court were to find that personal information has an inherent value and the deprivation of such value is an injury sufficient to confer standing, Plaintiffs have failed to allege facts indicating how the value of his personal information has decreased as a result of the Data Breach."); *Doe v. Meta Platforms, Inc*., 2023 WL 5837443 at *15-17 (in analyzing whether the plaintiffs had been damaged in their "property" under the UCL, the court dismissed the plaintiffs' UCL claim "in light of the inconsistent allegations regarding how plaintiffs could *and* would participate in a legitimate market for health care information.") (emphasis original); *Moore v. Centrelake Med. Grp., Inc.*, 83 Cal. App. 5th 515, 538 (2022), review denied (Dec. 14, 2022) (in determining whether the plaintiffs had been damaged in their "property" under the UCL, the court held the plaintiffs' did not have UCL standing because "[t]hey did not allege they ever attempted or intended to participate in this market, or otherwise to derive economic value from their PII. Nor did they allege that any prospective purchaser of their PII might learn that their PII had been stolen in this data breach and, as a result, refuse to enter into a transaction with them, or insist on less favorable terms.").

## IV. CONCLUSION

Because amendment would be futile, Overlake respectfully asks the Court to grant its motion to dismiss the Complaint with prejudice.

//

//

//

//

//

//

//

//

//



BAKER & HOSTETLER LLP
999 Third Avenue, Suite 3900
Seattle, WA 98104-4076
Telephone: (206) 332-1380

DATED this 5th day of October, 2023.

*s/ James R. Morrison*
James R. Morrison, WSBA No. 43043
Alexander Vitruk, WSBA No. 57337
Logan F. Peppin, WSBA No. 55704
BAKER & HOSTETLER LLP
999 Third Avenue, Suite 3900
Seattle, WA 98104-4076
Phone: (206) 332-1380
E-mails: jmorrison@bakerlaw.com
avitruk@bakerlaw.com
lpeppin@bakerlaw.com

Paul G. Karlsgodt, WSBA No. 40311
Baker & Hostetler LLP
1801 California Street, Suite 4400
Denver, CO 80202
Tel: (303) 861-0600
Fax: (303) 861-7805
E-mail: pkarlsgodt@bakerlaw.com

*Attorneys for Defendant*

*I certify that this document contains 8,103 words, in compliance with the Local Civil Rules.*

**CERTIFICATE OF CONFERRAL**

Consistent with the Court's Standing Order, Section II(D) Alexander Wolf, counsel for Plaintiff Jacq Nienaber and Alexander Vitruk and myself, counsel for Overlake, engaged in a Zoom meet-and-confer on September 29, 2023 in order to thoroughly discuss the substance of Overlake's contemplated motion to dismiss. Counsel thoroughly discussed the substance of the contemplated motion but the parties were unable to come to a resolution.

*s/ James R. Morrison*
James R. Morrison



BAKER & HOSTETLER LLP
999 Third Avenue, Suite 3900
Seattle, WA 98104-4076
Telephone: (206) 332-1380

**CERTIFICATE OF SERVICE**

I hereby certify that on October 5, 2023, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the following:

Andrew A. Lemmon
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN PLLC
16212 Reitan Road NE
Bainbridge Island, WA 98110
E-mail: alemmon@milberg.com

☒ Via e-Service
☒ Via Email
☐ Via Hand-Delivery
☐ Via Overnight Courier
☐ Via U.S. Mail

Gary M. Klinger
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
E-mail: gklinger@milberg.com

☒ Via e-Service
☒ Via Email
☐ Via Hand-Delivery
☐ Via Overnight Courier
☐ Via U.S. Mail

*Attorneys for Plaintiff and the Putative Class*

DATED: October 5, 2023

*s/ Pear Brown*
Pear Brown, Legal Assistant
Email: pebrown@bakerlaw.com